UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/509,125	03/28/2005	Shinichi Nakai	26379U	3318

20529 7590 11/10/2009

THE NATH LAW GROUP
112 South West Street
Alexandria, VA 22314

EXAMINER	
PHAM, LUU T	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
11/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/509,125	NAKAI ET AL.	
	Examiner	Art Unit	
	LUU PHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-49,67-69 and 87-93* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-49,67-69 and 87-93* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 07/27/2009.

2. In the instant Amendment, claims 1-46, 50-56, and 70-76 were previously cancelled; claims 47, 67-68, 87-88, and 90 have been amended; claims 47, 67, 87, and 90 are independent claims. Claims 47-49, 67-69, and 87-93 have been examined and are pending.

This Action is made FINAL.

Response to Arguments

3. The rejections of claims 47-49, 67-69, and 87-89 under 35 U.S.C. § 112, second paragraph, are withdrawn as the claims have been amended.

4. Applicants' arguments in the instant Amendment, filed on 07/27/2009, have been fully considered but they are not persuasive.

Applicants' arguments:

a. Asano fails to disclose *"encrypting 'identification data' which has a smaller data amount than an 'apparatus identifier' using an 'apparatus identifier' in an encrypting section."*

b. Asano fails to disclose *"encrypting both content and the 'identification data' using the apparatus identifier."*

c. Asano fails to disclose *using 'encrypted identification data' for selecting 'encrypted content' available to a specific content processing apparatus."*

The Examiner disagrees for the following reasons:

a. The combination of Asano and Hatakeyama does disclose 'identification data' has a smaller data than an 'apparatus identifier' *(Asano: pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; device identifier IDdev is known as apparatus identifier and signature key Kdev and/or integrity-check-value ICVs are known as identification data; device identifier has arbitrary length whereas Kdev and ICVs, computed by a hash function, have fixed length output (e.g., 128 bit output if using MD5 or 160 bit output if using SHA-1))* and encrypting 'identification data' using 'apparatus identifier' in an encrypting section *(Hatakeyama: col. 12, lines 38-48; col. 16, lines 38-65, and col. 18, lines 14-35; Figs. 6 and 14; licenses 84 to 86 are encrypted by the corresponding physical element IDs)*.

b. The combination of Asano and Hatakeyama does disclose encrypting both content and the 'identification data' using the apparatus identifier. Asano does disclose encrypting content using the 'apparatus identifier' *(Asano: pars. 0884-0890 and 0925; Figs. 69-70 and 78-79; data is encrypted using cryptography key Ksav, wherein Ksav could be the device ID; Ksav=recoding and reproducing device ID (IDdev) or DES[MKx, recording and reproducing device ID (IDdev)])*.
Hatakeyama does disclose encrypting 'identification data' using the 'apparatus identifier' *(Hatakeyama: col. 12, lines 38-48; col. 16, lines 38-65, and col. 18, lines 14-35; Figs. 6 and 14; licenses 84 to 86 are encrypted by the corresponding physical element IDs)*.

c. Asano does disclose 'encrypted identification data' for selecting 'encrypted content' available to a specific content processing apparatus *(Asano: pars. 0129, 0480-0491, 0560-0564, 0584-0586, 0644-0668, 0771-0775; Figs. 18-19, 22; Kdev and ICVs are used for verification and integrity check of the encrypted data; the system needs to select and locate the encrypted content before performing verification and integrity check)*;

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. **Claims 47-49, 67-69, 87-88, and 90-92 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Asano et al., (hereinafter "Asano"), U.S. Patent Publication No. 2002/0169971, published on November 14, 2002, in view of Hatakeyama et al., (hereinafter "Hatakeyama"), U.S. Patent No. 6,873,975, filed on March 08, 2000.

- **Regarding claim 47**, Asano discloses a content processing apparatus *(Figs. 2-3)* comprising:

a first storage section that stores therein an apparatus identifier unique to the content processing apparatus *(pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; recording and reproducing device identifier, IDdev, is stored in the memory of the recording and reproducing device 300)* and identification data which is different from the apparatus identifier and has a smaller data amount than the apparatus identifier *(pars. 0494-0496, 0773, and 0884-0885; Figs. 18-19, 49, and 69; recording and reproducing device signature key Kdev and integrity-check-value ICVs, stored in the memory of the recording and reproducing device 300, are known as identification data)*

an encrypting section that encrypts content [[and the identification data]] using the apparatus identifier *(pars. 0884-0890 and 0925; Figs. 69-70 and 78-79; data is encrypted using cryptography key Ksav, wherein Ksav could be the device ID; Ksav=recoding and reproducing device ID (IDdev) or DES[MKx, recording and reproducing device ID (IDdev)])*; and

an output section that stores the encrypted content and [[the encrypted]] identification data in the content storage medium which is detachable from the content processing apparatus *(pars. 0480-0491, 0560-0564, 0584-0586, 0644-0668, 0771-0775, and*

0884-0890; Figs. 19, 49, and 69; encrypted data and Kdev/ICVs are transmitted and stored in the recording devices 400A and 400B), wherein the encrypted identification data is used for selecting the encrypted content available to a specific content processing apparatus *(pars. 0129, 0480-0491, 0560-0564, 0584-0586, 0644-0668, 0771-0775; Figs. 18-19, 22; Kdev and ICVs are used for verification and integrity check of the encrypted data)*;

Asano does not explicitly disclose an encrypting section that encrypts the identification data using the apparatus identifier; and an output section that stores encrypted identification data.

However, in an analogous art, Hatakeyama discloses a content usage control system, including an encrypting section that encrypts the identification data using the apparatus identifier *(Hatakeyama: col. 12, lines 38-48; col. 16, lines 38-65, and col. 18, lines 14-35; Figs. 6 and 14; licenses 84 to 86 are encrypted by the corresponding physical element IDs);* and an output section that stores encrypted identification data *(Hatakeyama: col. 12, lines 38-48; col. 16, lines 38-65, and col. 18, lines 14-35; Figs. 6 and 14; licenses 84-86 are stored in license server 40; licenses 84-86 are sent to the user system 50)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Hatakeyama with the method and system of Asano with the system and method of Asano to include an encrypting section that encrypts the identification data using the apparatus identifier and an output section that stores encrypted identification data to provide users with a means for preventing illegal use of the content with high accuracy *(Hatakeyama: col. 4, lines 63-65 to col. 5, lines 1-4)*.

- **Regarding claim 48**, Asano and Hatakeyama disclose the content processing apparatus according to claim 47.

Asano further discloses an authentication section that determines whether access is allowed to a first area of the content storage medium *(Asano: pars. 0565, 0580-0591, 0979-0982, and 0985; Figs. 22, 28, and 87-88; wherein at least steps S52-S674, S79-S84, S907-909, and S927-S930)*, the content storage medium having the first area and a second area, wherein the output section stores the identification data encrypted in the first area, and stores the content encrypted in the second area *(Asano: Figs. 18-19, 32-35, 49, and 69)*.

- **Regarding claim 49**, Asano and Hatakeyama disclose the content processing apparatus according to claim 47.

Asano further discloses a second storage section that stores therein a title of the content, in association with the identification data *(pars. 0790-0805 and 0884-0885; Figs. 53-55 and 69; the medium ID may be unique to individual media, the titles of contents such as movies, or individual medium manufacturing lots)*.

- **Regarding claim 67**, Asano discloses a content processing apparatus *(Figs. 2-3)* comprising:

an input section that reads out encrypted content from a content storage medium which is detachable from the content processing apparatus, and encrypted first identification data from the content storage medium *(pars. 0374-0390, 0767-0782, and 0884-0913; Figs. 3-4, 49, and 69, read section 304 reads data including encrypted content, encrypted block information table, encrypted key data, content ID and usage policy, on the medium 500)*, wherein the encrypted first identification data is used for selecting the encrypted content

available to a specific content processing apparatus *(pars. 0129, 0480-0491, 0560-0564, 0584-0586, 0644-0668, 0771-0775; Figs. 18-19, 22; Kdev and ICVs are used for verification and integrity check of the encrypted data)*;

a first storage section that stores therein and an apparatus identifier unique to the content processing apparatus *(pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; recording and reproducing device identifier, IDdev, is stored in the memory of the recording and reproducing device 300)* and second identification data which is different from the apparatus identifier *(pars. pars. 0494-0496, 0773, and 0884-0885; Figs. 18-19, 49, and 69; recording and reproducing device signature key Kdev and integrity-check-value ICVs, stored in the memory of the recording and reproducing device 300, are known as identification data)* and has a smaller data amount than the apparatus identifier *(pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; device identifier IDdev is known as apparatus identifier and signature key Kdev and/or integrity-check-value ICVs are known as identification data; device identifier has arbitrary length whereas Kdev and ICVs, computed by a hash function, have fixed length output (e.g., 128 bit output if using MD5 or 160 bit output if using SHA-1))*.

a decoding section that decodes the encrypted first identification data [[using the apparatus identifier]] *(pars. 0539-0548, 0573-0592, and 0647-0681, and 0718-0728; Figs. 3, 22, 28, and 39-45; wherein at least steps S55, S74, S106, S161, and S207; cryptography process section decrypts encrypted block information table and encrypted key data)*; and

a comparing section that compares the decoded first identification data with the second identification data stored in the first storage section *(pars. 0539-0548; Figs. 22, 28,*

and 39-45; wherein at least steps S55-S56, S74-S75, S107-S109, and S207-S210; comparing ICVs after decrypting block information table),

wherein when the first identification data agrees with the second identification data, the decoding section decodes the encrypted content *(pars. 0580-0587, 0657-0660, 0708-0709; Figs. 22, 28, and 39-45; wherein at least steps S59-S63, S82, S114, and S219)* using the apparatus identifier *(pars. 0900-0903 and 0958-0961; Figs. 69, 72, 77, 79, and 85; steps S715, S776, and S836, decrypting save data with save data decryption key Ksav, wherein Ksav=IDdev (device identifier))*.

Asano does not explicitly disclose decoding the encrypted first identification data using apparatus identifier.

However, in an analogous art, Hatakeyama discloses a content usage control system including step of decoding the encrypted first identification data using apparatus identifier *(Hatakeyama: col. 16, lines 43, 65; col. 18, lines 65-67 to col. 19, lines 1-11; Figs. 6, 14, and 20-21; the content usage request are decoded based on the ID information of the physical elements of the content usage apparatus thereby to determine the license conditions)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Hatakeyama with the method and system of Asano with the system and method of Asano to include steps of decoding the encrypted first identification data using apparatus identifier to provide users with a means for preventing illegal use of the content with high accuracy *(Hatakeyama: col. 4, lines 63-65 to col. 5, lines 1-4)*.

- **Regarding claim 68**, claim 68 is similar in scope to claim 48, and is therefore rejected under similar rationale.

- **Regarding claim 69**, Asano and Hatakeyama disclose the content processing apparatus according to claim 67.

Asano further discloses a second storage section that stores therein a title of the content corresponding to the second identification data *(Asano: pars. 0790-0805 and 0884-0885; Figs. 53-55 and 69; the medium ID may be unique to individual media, the titles of contents such as movies, or individual medium manufacturing lots)*; and

a display section that displays the title stored in the second storage section *(Asano: pars. 0790 and 0863-0867; Figs. 53, 62, and 64, steps S671 and S675)* when the comparison of the comparing section indicates that the first specific identification data agrees with the second identification data stored in the first storage section *(pars. 0539-0548; Figs. 22, 28, and 39-45; wherein at least steps S55-S56, S74-S75, S107-S109, and S207-S210)*.

- **Regarding claim 87**, Asano discloses a content processing apparatus *(Figs. 2-3, 49, and 69)* that, in an information management system where digitized information of content is managed as a file on a detachable content storage medium and use of the digital information is allowed only in an environment providing a specific identifier, writes the digital information into the content storage medium *(Figs. 49, 69, 87, 88, and 90)*, the content processing apparatus comprising:

a first storage section that stores an apparatus identifier unique to the content processing apparatus *(pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; recording and reproducing device identifier, IDdev, is stored in the memory of the recording*

and reproducing device 300), and a identification data which is different from the apparatus identifier *(pars. pars. 0494-0496, 0773, and 0884-0885; Figs. 18-19, 49, and 69; recording and reproducing device signature key Kdev and integrity-check-value ICVs, stored in the memory of the recording and reproducing device 300, are known as identification data)* and has a smaller data amount than the apparatus identifier *(pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; device identifier IDdev is known as apparatus identifier and signature key Kdev and/or integrity-check-value ICVs are known as identification data; device identifier has arbitrary length whereas Kdev and ICVs, computed by a hash function, have fixed length output (e.g., 128 bit output if using MD5 or 160 bit output if using SHA-1)).*

an encrypting section that encrypts the content using the apparatus identifier [[and encrypts the identification data using the apparatus identifier]] *(pars. 0884-0890 and 0925; Figs. 69-70 and 78-79; data is encrypted using cryptography key Ksav, wherein Ksav could be the device ID; Ksav=recoding and reproducing device ID (IDdev) or DES[MKx, recording and reproducing device ID (IDdev)])*; and

an output section that stores the encrypted content and [[the encrypted]] identification data in the content storage medium *(pars. 0480-0491, 0560-0564, 0584-0586, 0644-0668, 0771-0775, and 0884-0890; Figs. 19, 49, and 69; encrypted data and Kdev/ICVs are transmitted and stored in the recording devices 400A and 400B),* wherein the encrypted first identification data is used for selecting the encrypted content available to a specific content processing apparatus *(pars. 0129, 0480-0491, 0560-0564, 0584-0586, 0644-0668, 0771-0775; Figs. 18-19, 22; Kdev and ICVs are used for verification and integrity check of the encrypted data).*

Asano does not explicitly disclose an encrypting section that encrypts the identification data using the apparatus identifier; and an output section that stores encrypted identification data.

However, in an analogous art, Hatakeyama discloses a content usage control system, including an encrypting section that encrypts the identification data using the apparatus identifier *(Hatakeyama: col. 12, lines 38-48; col. 16, lines 38-65, and col. 18, lines 14-35; Figs. 6 and 14; licenses 84 to 86 are encrypted by the corresponding physical element IDs);* and output section that stores encrypted identification data *(Hatakeyama: col. 12, lines 38-48; col. 16, lines 38-65, and col. 18, lines 14-35; Figs. 6 and 14; licenses 84-86 are stored in license server 40; licenses 84-86 are sent to the user system 50)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Hatakeyama with the method and system of Asano with the system and method of Asano to include an encrypting section that encrypts the identification data using the apparatus identifier and an output section that stores encrypted identification data to provide users with a means for preventing illegal use of the content with high accuracy *(Hatakeyama: col. 4, lines 63-65 to col. 5, lines 1-4)*.

- **Regarding claim 88**, Asano and Hatakeyama disclose the content processing apparatus according to claim 87.

Asano and Hatakeyama further disclose the content storage medium comprises a first area for which authentication is required for access and a second area for which authentication is not required *(Asano: Figs. 20, 39-45, and 88; wherein at least steps S45, S101-102 and S201-S202)*;

the content processing apparatus further comprises an authentication section that determines whether access is allowed to the first area of the content storage medium *(Asano: pars. 0565, 0580-0591, 0979-0982, and 0985; Figs. 22, 28, and 87-88; wherein at least steps S52-S674, S79-S84, S907-909, and S927-S930)*; and

the output section stores the encrypted specific identification data in the first area and stores the encrypted content in the second area, wherein the encrypted content is associated with the identification data in association with the identification data *(Asano: Figs. 3, 18-19, 32-35, 49, and 69; content ID, usage policy, block information table, key data, and encrypted content are stored in the medium 500; device identifier IDdev, system signature key Ksys, and device signature key Kdev are stored in the memory 3001, whereas encrypted data are stored in memory 400A-400C)*.

- **Regarding claim 90**, Asano discloses a content processing apparatus *(Figs. 2-3, 49, and 69)* that, in an information management system where digitized information of content is managed as a file on a detachable content storage medium and use of the digital information is allowed only in an environment providing a specific identifier, writes the digital information into the content storage medium *(Figs. 49, 69, 87, 88, and 90)*, the content processing apparatus comprising:

an input section that reads out encrypted content and encrypted identification data stored in the content storage medium *(pars. 0374-0390, 0767-0782, and 0884-0913; Figs. 3-4, 49, and 69, read section 304 reads data including encrypted content, encrypted block information table, encrypted key data, content ID and usage policy, on the medium 500)*, wherein the encrypted first identification data is used for selecting the encrypted content

available to a specific content processing apparatus *(pars. 0129, 0480-0491, 0560-0564, 0584-0586, 0644-0668, 0771-0775; Figs. 18-19, 22; Kdev and ICVs are used for verification and integrity check of the encrypted data)*;

a first storage section that stores an apparatus identifier unique to the content processing apparatus *(pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; recording and reproducing device identifier, IDdev, is stored in the memory of the recording and reproducing device 300)*, and a identification data which is different from the apparatus identifier *(pars. pars. 0494-0496, 0773, and 0884-0885; Figs. 18-19, 49, and 69; recording and reproducing device signature key Kdev and integrity-check-value ICVs, stored in the memory of the recording and reproducing device 300, are known as identification data)* and has a smaller data amount than the apparatus identifier *(pars. 0494-0496, 0773, and 0884-0885; Figs. 19, 49, and 69; device identifier IDdev is known as apparatus identifier and signature key Kdev and/or integrity-check-value ICVs are known as identification data; device identifier has arbitrary length whereas Kdev and ICVs, computed by a hash function, have fixed length output (e.g., 128 bit output if using MD5 or 160 bit output if using SHA-1))*;

a second storage section that stores the content *(Figs. 18-19, 32-35, 49, and 69)*;

a decoding section that decodes the encrypted identification data read out from the content storage medium [[using the apparatus identifier]] *(pars. 0539-0548, 0573-0592, and 0647-0681, and 0718-0728; Figs. 3, 22, 28, and 39-45; wherein at least steps S55, S74, S106, S161, and S207; cryptography process section decrypts encrypted block information table and encrypted key data)*;

a comparing section that compares decoded identification data obtained by decoding the encrypted specific identification data with the identification data stored in the first storage section *(pars. 0539-0548; Figs. 22, 28, and 39-45; wherein at least steps S55-S56, S74-S75, S107-S109, and S207-S210; comparing ICVs after decrypting block information table)*,

wherein, when the decoded identification data agrees with the identification data stored in the first storage section *(pars. 0580-0587, 0657-0660, 0708-0709; Figs. 22, 28, and 39-45; wherein at least steps S59-S63, S82, S114, and S219)*, the decoding section decodes the encrypted content using the apparatus identifier *(pars. 0900-0903 and 0958-0961; Figs. 69, 72, 77, 79, and 85; steps S715, S776, and S836, decrypting save data with save data decryption key Ksav, wherein Ksav=IDdev (device identifier))*.

Asano does not explicitly disclose decoding the encrypted identification data using apparatus identifier.

However, in an analogous art, Hatakeyama discloses a content usage control system including step of decoding the encrypted identification data using apparatus identifier *(Hatakeyama: col. 16, lines 43, 65; col. 18, lines 65-67 to col. 19, lines 1-11; Figs. 6, 14, and 20-21; the content usage request are decoded based on the ID information of the physical elements of the content usage apparatus thereby to determine the license conditions)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Hatakeyama with the method and system of Asano with the system and method of Asano to include steps of decoding the

encrypted identification data using apparatus identifier to provide users with a means for preventing illegal use of the content with high accuracy *(Hatakeyama: col. 4, lines 63-65 to col. 5, lines 1-4)*.

- **Regarding claim 91**, Asano and Hatakeyama disclose the content processing apparatus according to claim 90.

Asano and Hatakeyama further disclose the input section reads out the encrypted identification data before reading out the encrypted content from the content storage medium *(Asano: pars. 0374-0390, 0767-0782, and 0884-0913; Figs. 3-4, 49, and 69, content ID usage policy, encrypted block information table, and encrypted key data are read before reading encrypted content)*;

the comparing section compares identification data obtained by decoding the encrypted identification data at the decoding section with the identification data stored in the first storage section and determines whether the decoded identification data agrees with the stored identification data *(Asano: pars. 0539-0548; Figs. 22, 28, and 39-45; wherein at least steps S55-S56, S74-S75, S107-S109, and S207-S210; comparing ICVs after decrypting block information table; Hatakeyama: col. 14, lines 25-65; col. 16, lines 12-65; Figs. 10 and 12-14)*; and

only when the decoded identification data is determined to agree with the stored identification data, the input section reads out the encrypted content from the content storage medium, and the decoding section decodes the encrypted content using the apparatus identifier *(Asano: pars. 0580-0587, 0657-0660, 0708-0709; Figs. 22, 28, and 39-45;*

wherein at least steps S59-S63, S82, S114, and S219; Hatakeyama: col. 16, lines 43, 65; col. 18, lines 65-67 to col. 19, lines 1-11; Figs. 6, 14, and 20-21).

- **Regarding claim 92**, Asano and Hatakeyama disclose content processing apparatus according to claim 90.

Asano and Hatakeyama further disclose the content storage medium comprises a first area for which authentication is required for access and a second area for which authentication is not required *(Asano: Figs. 20, 39-45, and 88; wherein at least steps S45, S101-102 and S201-S202)*;

the content processing apparatus further comprises an authentication section that determines whether access is allowed to the first area of the content storage medium *(Asano: pars. 0565, 0580-0591, 0979-0982, and 0985; Figs. 22, 28, and 87-88; wherein at least steps S52-S674, S79-S84, S907-909, and S927-S930)*; and

the input section reads out the encrypted identification data from the first area and reads out the encrypted data from the second area *(Asano: pars. 0374-0390, 0767-0782, and 0884-0913; Figs. 3-4, 49, and 69, read section 304 reads data including encrypted content, encrypted block information table, encrypted key data, content ID and usage policy, on the medium 500).*

8. **Claims 89 and 93 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Asano and Hatakeyama, as applied to claims 87 and 90 above, and further in view of Kontio, U.S. Patent Publication No. 2005/0004875, filed on March 12, 2002.

- **Regarding claim 89**, Asano and Hatakeyama disclose the content processing apparatus according to claim 87.

Asano and Hatakeyama do not explicitly disclose the content processing apparatus comprises a cellular telephone, and the apparatus identifier comprises a telephone number or a serial number of the cellular telephone.

However, in an analogous art, Kontio discloses method for controlling the distribution of digital assets, wherein the content processing apparatus comprises a cellular telephone, and the apparatus identifier comprises a telephone number or a serial number of the cellular telephone *(Kontio: pars. 0081 and 0263; Fig. 1; mobile phones 100 and 140; device IDs could be implemented using unique serial number)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kontio with the method and system of Asano and Hatakeyama, wherein the content processing apparatus comprises a cellular telephone, and the apparatus identifier comprises a telephone number or a serial number of the cellular telephone to provide users with a means for controlling the distribution of digital assets in communication networks *(Kontio: pars. 0002)*.

- **Regarding claim 93**, claim 93 is similar in cope to claim 89, and is therefore rejected under similar rationale.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information

about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437